

HIPAA TEMPLATE DRAFT

Title **Employee Confidentiality Acknowledgement**

Creation

- Date July 16, 2001
- Author Vonnie Behm, DMH
- Email Address www.dds.ca.gov/hippasecurity

Revision

- Date
- Author
- Phone Number
- Email Address

I. Introduction

This template is designed to provide documentation that the employer has provided training and has clearly communicated the employee's responsibility for maintaining both security and privacy protection and the sanctions for violations of those requirements. The attached Employee Confidentiality Acknowledgement is designed to provide documentation that the employee acknowledges that he or she has received the information related to the maintenance, disclosure, or destruction of confidential health information.

Confidentiality Acknowledgements should be read and executed by all Agency personnel and all vendor or business partner personnel with access to protected information.

Confidentiality Acknowledgements should sufficiently identify the type of information to be protected, the employee's responsibility to protect it, and methods to protect it in order to assure confidentiality and to comply with HIPAA regulations.

II. Purpose

Covered entities must have policies, procedures and systems in place to protect the confidentiality (or security) of health information and individual rights to privacy. Requirements include safeguards to prevent intentional or accidental misuse of protected health information and sanctions for employee violations of those requirements. A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information and must document that the training has been provided.

Reference: 45 CFR, Part 164, 164.530
45 CFR, Part 142, 142.308 (Proposed Rule)

III. Assumptions

Policies and procedures to protect health information will be in place for agency/department.

IV. Pre-requisites

Every agency must have in place a Confidentiality Acknowledgment for its own employees and for its vendors and business partners.

V. Constraints

Time

Any deadline on meeting compliance requirements

Personnel

Are there agency Security Officers? Who else has authority?

Resources

Materials

Facilities

Access

Authorities

Funding/ Budget

Personnel

Authorities

Security Officer

Privacy Officer

IT unit

Information Security Unit

VI. Dependencies

All vendors and business partners will have in place security measures to protect the information assets covered by HIPAA; these include, but are not limited to, systems, personnel, and equipment.

VII. Process and Procedures

A. A covered entity must provide training:

1. To each member of the covered entity's workforce by no later than the compliance date for the covered entity;
2. Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and
 - a. To each member of the covered entity's workforce and independent contractors whose functions are affected by a material change in the privacy or security policies or procedures within a reasonable period of time after the material change becomes effective.

Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

- B. A covered entity must document that the training has been provided. At a minimum, documentation of training shall consist of a signed acknowledgement by the member of the workforce specifying which training has been received and the date the training was taken.
- C. A covered entity must retain the documentation for six years from the date of its creation or the date when it last was in effect, whichever is later.
- D. A covered entity should maintain a training record for each member of its workforce. The training record should include the specific training and the dates the training was received and/or the signed acknowledgement referred to above in Item B. These training records will assist the covered entity in identifying where supplementary training needs to be conducted should there be changes in the privacy or security regulations.

VIII. Accessibility of information

The Agency shall make its records available for inspection by (INSERT: i.e., State Auditor, etc.) upon request for a period of (INSERT: number of years)

The Covered Entity or Business Partner shall make its records available to the Agency for a period of six years.

IX. Compliance criteria

The Covered Entity or Business Partner shall permit the Agency to make on-site inspections to ensure that the HIPAA regulations are followed and security measures are in place and in practice.

X. Enforcement

Roles and Responsibilities for the Agency/Department Information Security Officer and Privacy Officer should include monitoring and enforcement of the privacy and security procedures and requirements.

XI. Disclaimer

The information in this template is for general information only. It is not intended to provide legal advice to any entity. Please consult with your Legal Counsel before taking any action based on information appearing on this template.

EMPLOYEE CONFIDENTIALITY ACKNOWLEDGMENT

I understand that while performing my official duties I may have access to information that is classified as either confidential or sensitive or protected health information. Confidential information is information that identifies an individual or an employing unit. Sensitive information may be financial or operational information that requires the maintenance of its integrity and assurance of its accuracy and completeness. Protected Health Information (PHI) means individually identifiable health information that is transmitted or maintained in any form or medium. Confidential, sensitive, protected health information is not open to the public. Special precautions are necessary to protect this type of information from unauthorized access, use, modification, disclosure, or destruction.

I agree to protect the following types of information:

- Client information (such as, disability insurance claimants, recipients of public social services, participants of state/federal programs, employers, etc.)
- Wage earner information
- All data elements described as protected health information in HIPAA (Section 164.514)
- Information about how automated systems are accessed and operate.
- Any other proprietary information.
- Operational information (instructional manuals)

I agree to protect confidential and sensitive and PHI by:

- Accessing, using, or modifying confidential and/or sensitive and/or PHI only for the purpose of performing my official duties.
- Never sharing passwords with anyone or storing passwords in a location accessible to unauthorized persons.
- Never accessing or using confidential and/or sensitive and/or PHI out of curiosity, or for personal interest or advantage.
- Never showing, discussing, or disclosing confidential and/or sensitive and/or PHI to or with anyone who does not have the legal authority or the "need to know".
- Storing confidential and/or sensitive information in a place physically secure from access by unauthorized persons.
- Never removing confidential and/or sensitive and/or PHI from the work area without authorization.
- Disposing confidential and/or sensitive and/or PHI by utilizing an approved method of destruction, which includes shredding, burning, or certified or witnessed destruction. Never disposing such information in the wastebaskets or recycle bins.

Penalties

Unauthorized access, use, modification, disclosure, or destruction is strictly prohibited by state and federal laws, including but not limited to California Penal Code Section 502, California Civil Code Section 1798.53 or 1798.55 (for state and local governmental agencies), and California Unemployment Insurance Code 2111. The penalties for unauthorized access, use, modification, disclosure, or destruction may include disciplinary action and/or criminal or civil action.

The State reserves the right to monitor and record all network activity including e-mail, with or without notice, and therefore users should have no expectations of privacy in the use of these resources.

"I certify that I have read and understand the Confidentiality Statement printed above."

Print Full Name (first, middle initial, last)

Signature

Agency/Department

Date Signed

DRAFT FOR COMMENTS This is a HIPAA readiness document authored by the State HIPAA Workgroup. Information presented is accurate to the best of our knowledge. Information identified as related to or authored by someone other than the Workgroup has not been verified for accuracy. Unless noted otherwise, this is a working document. All material must be viewed in the context of your own organization and environment. Legal opinions or decision documentation may be needed to apply/interpret it.

Docum HIPAA_temp_emp_sec_010629

